Claims:

1. A method of enabling information exchange between a protected system and an external information source wherein the information is contained in a data set carried by a signal while preventing any undesired data from reaching the protected system comprising the steps of:

A. connecting an intermediate domain computer hardware device between an external data set source and the protected system to receive an initial data set including the information and any undesirable data transmitted from the external information source;

B. processing within the intermediate domain device the signal containing the initial data set to a second data set, wherein processing includes the execution of any programs contained in the initial data set;

C. extracting the information from the second data set to thereby screen out undesirable data;

D. passing the extracted information to the protected system;

E. eliminating the initial data set from the intermediate domain computer hardware device;

F. resetting the intermediate domain computer hardware device to a non-contaminated state; and

G. converting the extracted information to data sets that are optimally processable by the protected system.

2. The method of claim 1 wherein the processing step includes selecting an internal data set that is to react with the initial data set, transferring the internal data set to the intermediate domain device and thereafter processing the initial and internal data sets within the intermediate domain device thus confining undesirable data to the intermediate domain device and obtaining the second data set.

3. The method of claim 2 including the additional step of filtering the selected internal data set for authorized transfer to the intermediate domain device.

4. The method of claim 1 wherein the information processing step includes buffering the signal containing the initial data set in the intermediate domain device, and thus confining the initial data set within the intermediate domain device and transforming the format of the signal containing the initial data set into a different format.

5. The method of claim 4 in which the first and different formats are selected from a group of formats including analogue, digital, printed, telephone, video, optical, facsimile, media, text or font, EBCIDIC and ASCII and, other forms of electro-magnetic and electro-optic signals.

6. The method of claim 1 wherein the step of connecting includes connecting the

intermediate computer hardware device to a backplane of a computer system operating as the protected system.

7. A system for enabling information exchange between a protected system and an external information source when the information is contained in a data set carried by a signal while preventing any undesired data from reaching the protected system, the system comprising:

a) means for connecting an intermediate domain computer hardware device between an external data source and the protected system to receive an initial data set including the information and any undesirable data transmitted from the external source;

b) means for processing, within the intermediate domain device, the signals containing the initial data set so as to extract the information from the initial data set thus forming a second data set containing the information thereby screening out undesirable data, wherein means for processing includes the execution of any programs (i.e. executable code) contained in the initial data set;

c) means for securely passing the extracted information to the protected system;

d) means for purging the initial data set from the intermediate domain device;

e) means for resetting the intermediate domain device to a non contaminated state; and

f) means for converting extracted information to data sets optimally processable by the protected system.

8. The system of claim 7 wherein said intermediate domain device is selected from a group of computer hardware devices, including single board computers, modified single board computers, embedded microprocessors, embedded microcontrollers, personal computers, webtv units, portable/laptop computer systems, mainframe computers, network computer systems, network of computers, and a plurality of such devices, whereby a modified single board computer devise includes a "commercial of the shelf" (COTS) single board computer device modified to include an embedded "non-transparent" bus-bridge device which permits the single board computer to operate as an add-in card to the bus.

9. The system of claim 7 including means for identifying a protected system for authorized access to the intermediate domain device.

10. The system of claim 7 in which said means for connecting, means for processing, means for passing, means for purging, and means for resetting are mounted to a bus of the protected system.

11. The system of claim 7 including a plurality of intermediate domain computer hardware devices, and means for identifying authorized intermediate domain computer hardware devices in a network.

12. The system of claim 11 wherein the means for identifying includes a DIN authentication capability, and a data set labeling capability.

13. The system of claim 12 wherein the DIN authentication capability and the data set labeling capability includes means to tranceive and process patterns of information representing labeled data sets that appear as noise to unauthorized receivers, and which cannot be correctly generated by unauthorized transmitters.

14. The system of claim 13 wherein the means to tranceive is operable in a framework of a telecommunication medium and the means to process patterns includes adaptive processing means for removing limitations of binary computation.

15. The system of claim 7, wherein the means for connecting and means for processing include means to control a flow of signals including data sets to and from the system based on a DIN of the system and a label of the signals and wherein the DIN of the system is considered a label of the system.

16. The system of claim 7, wherein the means for connecting and means for processing includes means to derive a point of origin of signals received by the system.

17. The system of claim 16, wherein the means for connecting and means for processing includes means to authenticate contents of signals received by the system, when said received signals have been processed for transmission by the external

source.

18. The system of claim 7, wherein the means for connecting and means for processing includes means to process the data sets so as to be authenticated upon passing to the protected system and wherein the protected system includes means to authenticate the authenticated data sets.

19. The system of claim 7, wherein the protected system is a router, switch, hub, network device, wireless device, mobile device, or handheld device, wherein the means for processing and the means for securely passing include means to analyze both incoming and outgoing data sets so as to identify improper data sets, delete the improper data sets, and control the flow of the data sets to and from the protected system, whereby adverse operational impact on the protected system is minimized.

20. The system of claim 19, wherein means for processing and means for securely passing includes means to generate status information and tranceive such status information with a plurality of protected systems and analyze such status information for maintaining optimal passing of data sets.

21. The system of claim 19, wherein the means for connecting, means for processing, means for securely passing, means for purging/flushing, means for resetting, and means for converting are imbodied as a system-on-chip (SOC) device,

wherein such (SOC) device includes mixed-signal components, wireless technology, application specific integrated circuit (ASIC) devices, and reconfigurable logic unit (RLU) devices which provide fault-tolerant capability and reconfigurable-computing capability to the system-on-chip device.

09865454 .052901